SECTION 7
DATA MANAGEMENT

QUESTIONS THIS SECTION WILL ANSWER	Para.
1. What is the relationship between configuration management and data management?	7.1
2. What principles of CM apply to the management of data?	7.2
3. How does the conceptual schema in MIL-STD-2549 satisfy each of the above principles?	7.2.1-7.2.6, 7.3
4. Is there any difference between configuration documentation and other technical data with regard to how it is managed?	7.1
5. What digital data attributes are essential for an effective Government/contractor data interface?	7.2, 7.3
6. What factors need to be considered when acquiring CM data from a contractor?	7.3

7.1 CM Related Data Management Activity

In this age of rapidly developing information technology, data management and particularly the management of digital data is an essential prerequisite to the performance of configuration management. Digital data is information prepared by electronic means and made available to users by electronic data access, interchange, transfer, or on electronic/magnetic media. There is virtually no data today, short of handwritten notes, that does not fall into this category. Configuration management of data is therefore part of data management activity; and management of the configuration of a product configuration cannot be accomplished without it.

Figure 7-1 is an activity model for configuration management of data. All of the activities shown apply to configuration documentation. Most of the activities apply to all data. The model illustrates that the process is driven by business rules established based on the Contractor process as adjusted to accommodate the Government’s concept of operations for the processing of digital data, and specific contract data requirements. It assumes a data workflow that encompasses four progressive status categories of digital data files.

- Working data, where the data is under the originator's control only
- Released data, where working data has been approved by the contractor's established approval process, released for its intended use, and is now subject to contractor configuration control procedures
- Submitted data, where contractor released data has been formally submitted to the Government for approval
- Approved data, where contractor submitted data has been approved for its intended use by the Government

When the data process is initiated to create or revise an item of data, or to perform any of the actions necessary to bring it from one status level to the next, the various rule sets illustrated in the figure are triggered to facilitate the work flow. The result is a data product with:

- Appropriate document, document representation and data file identification,
- Version control,
- Clear and unambiguous relationships to the product configuration with which it is associated, and to the changes which delineate each configuration of the product

In addition, the data is available for access in accordance with contractually agreed to rules for submittal, transmission, or on-line access (as appropriate), in the prescribed format (document representation) that can be used by the application software available to the authorized user.

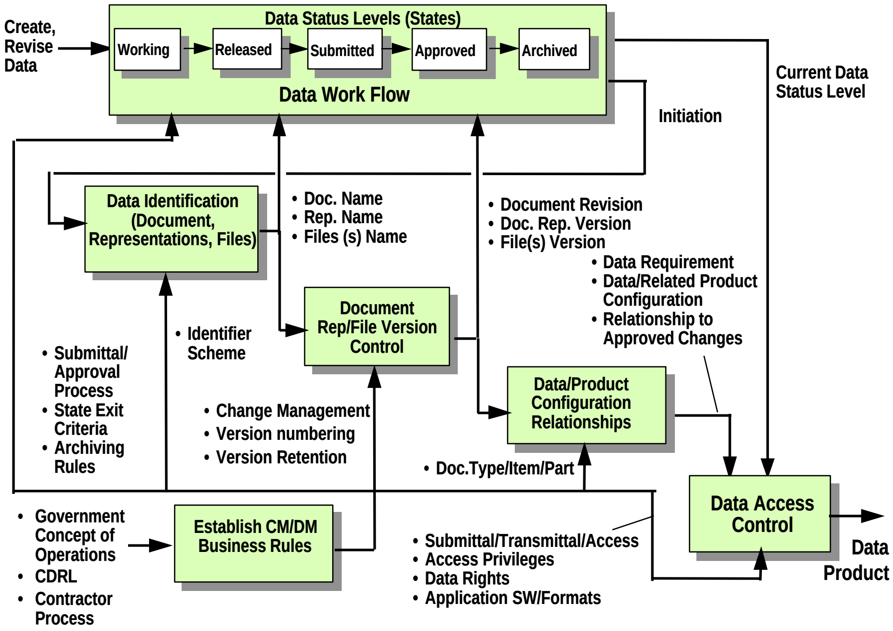

Figure 7-1. CM Related Data Management Activity Model

7.2 CM Related Data Management Concepts and Principles

Configuration management principles ensure the integrity of digital representations of product information and other data and enhance good data management practice. The concepts are described, as follows, based on elements and principles expressed in **EIA Standard 649**:

- Document identification
- Data status level management
- Data and product configuration relationships
- Data version control and management of review, comment, annotation, and disposition
- Digital data transmittal
- Data access control.

7.2.1 Document Identification

Each document reflecting performance, functional, or physical requirements or other product related information must be given a unique identifier so that it can be

- Correctly associated with the applicable configuration (product identifier and revision) of the associated item.
- Referred to precisely
- Retrieved when necessary.

With emphasis on the acquisition of commercial products and the use of industry methods, it is inappropriate for the military to specify one format for document identifiers. Except for MIL documents and program unique specifications, whose identifiers are governed by **MIL-STDs-961 - 963**, document identifier formats are determined by the document originators. Generally they include all or most of the following parameters:

- Date
- Assigned numeric or alpha numeric identifier unique to the document
- Revision indicator
- Type of document
- Title or subject
- Originator/Organization

This listing is substantiated by the following business rule for document identification in **MIL-STD-2549,: [Detail: Figure 7-3. Activity Guideline: Generic Document Identification]**

A document iteration is uniquely identified by a combination of

- Document source (CAGE code, organizational acronym, or company name)
- Document identifier (Number or title)
- Document type (Refer to **MIL-STD-2549 Appendix C, DED 0004**)
- Revision indicator (Letter, number or date)

A document is digitally represented by one or more electronic data files. Each document representation is the complete set of all the individual digital data files (e.g., word processor, CAD/CAM , graphics, database, spreadsheet, software) constituting one document.

As shown in **Figure 7-2**, the same document can have several different, equally valid, representations such as different word processing or standard neutral formats (IGES, ASCII, SGML-tagged ASCII,). Any individual file such as a raster graphics file, an ASCII file, or a spread sheet file may be part of several document representations of the same document/same revision; same document/different revision, or different document. The business rules defined in **MIL-STD-2549** relating documents, documentation representations and files are as follows:

1. Each document iteration exists as one or more document representations, identified by:
    - Document identifier
    - Document representation identifier
    - Document representation revision identifier

2. Each document representation is comprised of zero or more files

To facilitate the proper relationships, apply the following digital data identification rules to maintain document, document representation, and file version relationships.:

- Assign a unique identifier to each file
- Assign a unique identifier to each document representation
- Assign a version identifier to each file
- Maintain, in a database, the relationship between:
    - Document identifier and its revision level
    - Associated document representation(s)
    - File identifiers and versions
    - Retain multiple versions of files as necessary to recreate prior document revisions and provide a traceable history of each document
- Identify the tool, and version of the tool (e.g., msword 97) used to generate the document when the document is not in neutral format.

7.2.2 Data Status Level Management

Document status level **[See 7.1]** is important as a foundation for the business rules defining access, change management, and archiving of digital data documents. It is the basis for establishing data work flow management and enhances data integrity **[Refer back to Figure 7-1]** The standard data life cycle model shows the data status levels (also referred to as states) that a specific document/document revision is processed through in it’s life cycle.

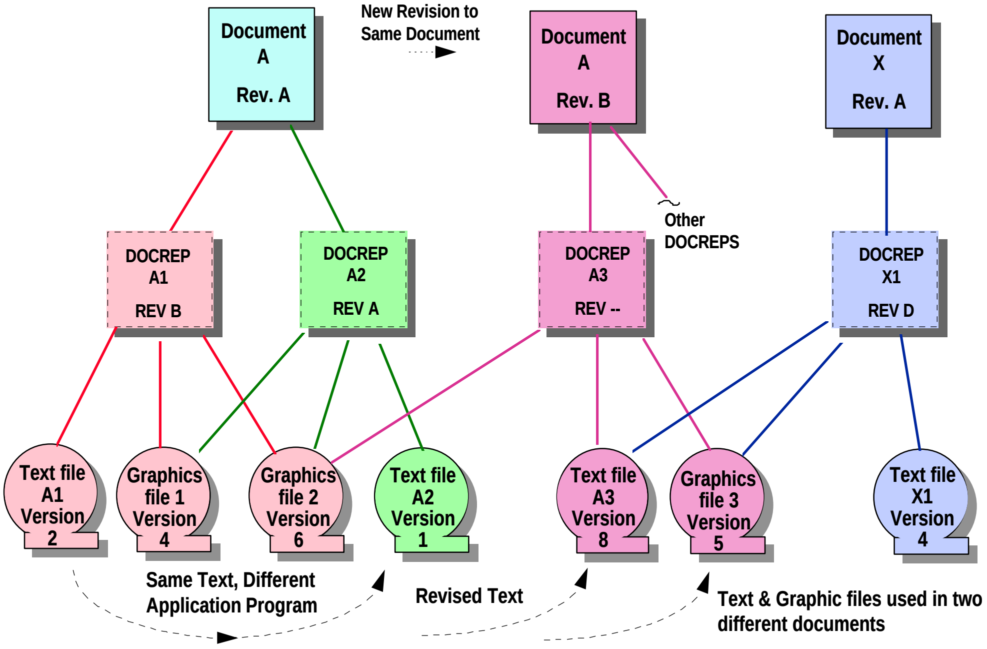

Figure 7-2. Illustration of Document Representation Concepts

These levels were initially defined in MIL-HDBK-59A (CALS Handbook, now cancelled). They were also defined in MIL-STD-974 "Contractor Integrated Technical Information Services (CITIS)" and in EIA Standard 649. The intent of the definitions in those documents has been preserved in MIL-STD-2549; however, the requirements of a precise data model have necessitated a number of enhancements to the concept and therefore a modification to the definitions. ***The key change is the concept of one or more document representations, and revisions thereto, for each document and document revision (see 7.2.1).*** The MIL-STD-2549 definitions of data status terms follow; the key changes from the previous definitions are highlighted and rationale for the differences is provided in the attendant footnotes:

- Working is the status used to identify data (***document representations*** [1] ***or document revisions***) that are in preparation - a work in progress that is subject to unilateral change by the originator. Each design activity may define any number of subordinate states within the working category, to define the unique processes that different document types go through before release in their organization.
- Released is the ***status of document representations, and revisions thereto,*** that have been reviewed and authorized for use or for submittal to, or access by, a customer (for example, the Government) or supplier. Released data are under originating organization (for example, a contractor) change management rules, which means that a new revision of the document representation cannot replace a released revision of a document representation until it has also been reviewed and authorized by the appropriate authority. ***The content of a document representation revision is fixed, once it is in the released state. It is only changed by release of a superseding document representation revision. Once a document (or document revision) is in the approved state, changes are made only by release of a new document representation related to the next document revision .***[2]
- Submitted data is either an ***approved document revision, or a proposed document revision with released document representation,*** which has been made available for customer review. This status applies only to data that requires submittal to or access by a customer (usually the Government).

[1] This change to the definition of working status recognizes the fact that there can be multiple representations of a document revision.

[2] This change to the definition of released status reserves the status of released for document representation revisions rather than document revisions. It allows the enterprise to release and iterate document representations without changing the document revision. Thus representations of proposed revisions to Rev A of a document may be reviewed, revised and reissued several times before a satisfactory Rev B (document) is issued.

1. If a submitted document revision, ***which has not been approved***, is commented to, or disapproved, a new working revision of the related document representation may be started and eventually ***replace the original document representation*** without affecting the identifier proposed for the new document revision.
2. If a submitted document revision ***which has been approved*** is commented to, or disapproved by the customer, a new working ***representation of the next document revision*** may be started and eventually ***replace the original document revision.*** [3]

- Approved is the status of documents and document revisions signifying that the data ***(document revision) has been approved by the CDCA of the document. The content of a document revision is fixed, once it is in the approved state.*** It is only changed by approval of a superseding document revision.
- Some tools which implement CM AIS include Archived as a data status for document representations and/or documents [4] This status is independent of the approval status (released, submitted, and approved) and ***merely means that has the data been removed from an active access storage mode***. [5]

No changes are allowed in the document representations that progress to the released state, or in document revisions that progress to the approved state. If there are changes to be made, they are accomplished by the generation and release or approval of a new revision. Documents must have at least one released document representation in order to be approved by the CDCA or submitted to a non-CDCA customer for review and adoption. Some data will exist only at the working level.

Business rules related to document/data status apply to each document type by defining requirements such as the following:

- Whether submittal to (or access by) customer(s) is required
- In which application software and data format is submittal/access required
- Who will be granted access privileges to the data in each of the applicable states
- What are the approval requirements (reviewers/approvers) and method of approval (e.g., electronic signature) to promote a document to the released state; the approved state
- What are the archiving rules for this document type (e.g., all released versions upon release of a superseding version, all released versions, 90 days after release of a superseding version, etc.)?

7.2.3 Data and Product Configuration Relationships

A product data management system must provide an effective system to maintain the key relationships between digital data, data requirements, and the related product configuration so that the correct revision of an item of data can be accessed or retrieved when needed. Data files are related to documents via document representations. **[Section 7.2.1]** Each product document, with a specific source, document type, document identifier (title, name and number) and document revision identifier, may have the following relationships:

- Program/project and/or contractual agreement
- Contract data item identifiers
- Document revision/change authorization
- Associated product (hardware or software) name
- Associated product (end item), part or software identifying number and revision/version identifier, where applicable

[3] This change to the definition of submitted recognizes that there are two conditions that apply to submitted data, approved data (see definition) and un-approved data. It also applies the concept discussed in footnote 2. The MIL-STD-2549 document approval paradigm does not put submitted sequentially after released. If the contractor is the CDCA, it may approve before submitting; it may approve without submitting, it may release a document representation as a draft of the new revision and submit it for review before approving the document. If the contractor is not the CDCA, it must release a document representation before submitting it to the CDCA for approval of the document revision.

[4] As did MIL-HDBK-59, MIL-STD-974, and EIA-649

[5] The revisions to the archived status definition simply recognize that archived is an indicator of the location of the data rather than a true status indicator. Archived is a tool/memory dependant condition that is not part of the MIL-STD-2549 conceptual schema.

- The effectivity in terms of end item serial numbers for the associated product, part, software item
- Status (working, released, submitted, approved, archived) of the data **[7.2.2]**
- Associated data - document name/document title/document revision number and date
- Associated correspondence - document number, subject, date, references

The business rules for document retrieval should use these key relationships within a database to assure the integrity of the data that users may extract. Thus information concerning a given product or part is associated with the configuration and effectivity (serial number) of the end item that uses the part. This capability is particularly significant during the operation and support phase, when data is needed to support maintenance activity and to determine the appropriate replacement parts for a specific end item.

7.2.4 Data Version Control

Disciplined version control of data files is the prerequisite to effective electronic management of digital documentation and must be encompassed within the product data management software. Version identification **[See 7.2.1]** occurs whenever a file is changed. The simplest form of version management is the file save feature incorporated in application software which advances the file date and time identification each time a file is saved. However to retain the superseded version, it must be renamed. True version control business rules require automatic version identifier advance whenever a file is revised and not when the file is saved without change. Furthermore, they require all versions to be retained, subject to archiving guidelines and special rules pertinent to specific document types.

Since a single document representation can consist of many files, a very disciplined process is necessary to manage a document review process electronically. Version control rules facilitate the establishment of an audit trail of comments and annotations by reviewers, and the disposition of each comment. Each version of each document representation provided to, or received from, each reviewer is uniquely identified and associated with the source of the comment. Essentially this means that a reviewer’s version of a set of files (document representation) constituting a document being reviewed is re-named to enable the annotated comment copy to be distinguished from the official current version of the document. **[Detail: Refer to EIA-649]**

7.2.5 Digital Data Transmittal

Part of the obligation of the sender of any document, regardless of transmission method is to make sure that the document is in a format (document representation) that can be read by the receiver and converted to human readable form. Appropriate identification is affixed to media physical media such as floppy disks or tapes to clearly identify its contents. If all of the file identifications cannot be included on the label, a directory, reference to an accompanying listing or to a read.me file is used.

EIA-STD-649 lists the following the following common sense guidelines for information to be provided to the user (via such means as "read.me" files, reference to standard protocols, on-line help), where applicable:

✓ Identification of the files included in the transfer by file name, description, version, data status level, application/file type and application version.
✓ Applicable references to associate the data with the basis (requirement) for its transmittal, approval, and payment, where applicable
✓ If there are multiple files, such as separate text and graphics, how to assemble each included data item for reading, review or annotation, as applicable
✓ The naming convention for file versions and data status level which distinguishes altered (For example, annotated or red-line/strike-out) file versions from unaltered files.
✓ If and how changes from previous versions are indicated
✓ How to acknowledge receipt of the data, provide comments, and/or indicate disposition of the data digitally
✓ Time constraints, if any, relating to review and disposition.

7.2.6 Data Access Control

Access to digital data involves retrieving the appropriate files necessary to compile the correct version of each digital data document, view it, and perform the prescribed processing. Seeking digital data access should be as user-friendly as possible. Users should be provided with data/documents they are entitled to in the correct revision/version. Before this can be accomplished, there are a number of pertinent parameters concerning access privileges, security and protection of data rights that must be set-up.

Access privileges limit access to applicable users. Access privileges vary according to the individuals credentials (security clearance, need to know, organizational affiliation, etc.), data status level, the document type, program milestones, and the user need predetermined from the Government's concept of operations. Users of accessed data must respect all contractual and legal requirements for data rights, security, licenses, copyrights, and other distribution restrictions which apply to the data The applicable distribution code, which represents the type of distribution statement, must be affixed to a document or viewable file to indicate the authorized circulation or dissemination of the information contained in the item. **[Ref: MIL-STD-2549, Appendix C, DED 0014]**

Typically, working data should be made available only to the originating individual, group, or team (such as an integrated product development team); or to other designated reviewers of the data. If the Government is a direct participant in the team, the Government team members should be afforded the same access as the other members. In plant Government representatives have the right to request any and all data generated as part of the contract to which they have oversight responsibility; the contractor can determine the means of providing that access. With these exceptions, Government access to digital data (including data retrieved from databases) should be limited to contractually stipulated released, submitted, and approved data.

EIA-STD-649 provides us with the following checklist of ground rules to be pre-established prior to initiating interactive access (i.e., pre-defined query and extraction of data):

- ✓ How data is to be accessed
- ✓ Request for access and logging of access for read-only or annotation
- ✓ Naming of temporary working version of the file(s) for purpose of annotation/mark up
- ✓ Means of indicating whether a comment/annotation is essential/suggested
- ✓ Re-identification of marked up versions, as required
- ✓ Method of indicating acceptance, approval, or rejection, as applicable
- ✓ Time constraints, if any, on data acceptance
- ✓ Tracking of disposition of required actions
- ✓ Re-identification of changed files.

7.3 Data Management Activity Guides

7.3.1 Document Identification

Figure 7-3 which is a diagram of the generic document identification schema in **MIL-STD-2549** provides guidance in understanding the possible data identification relationships that the Government can expect to see when dealing with a variety of document originating from many different sources. Each document is identified uniquely by the combination of its source, its identifier, and its document type. A document identifier can include a number and a title, or either a number or a title. A numbered document may have a CAGE code, a company name, or an organizational acronym identifying its source. Certain document types are associated with each type of source.

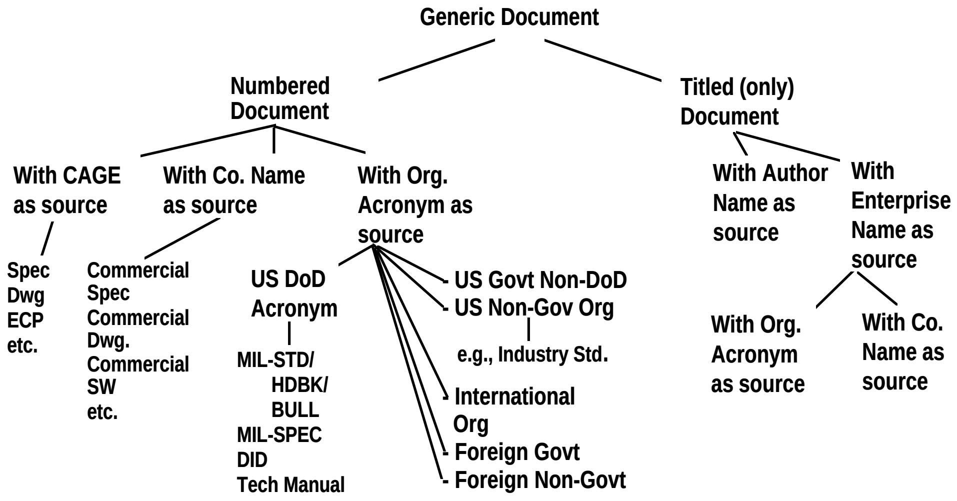

Figure 7-3. ***Activity Guide*****: Generic Document Identifier Characteristics**

7.3.2 Configuration Management Data Acquisition Guidance

This section provides details on the actions required to define digital data for delivery to or access by the Government in general, and for configuration management data in particular. With interactive access, the emphasis is on Government access to contractor maintained data bases. It is most important to precisely define the requirements for digital data in the Contract data Requirements List (CDRL). **Figure 7-4** and **Table 7-1** models and provide explanation of the factors involved in defining a CDRL item for digital data.

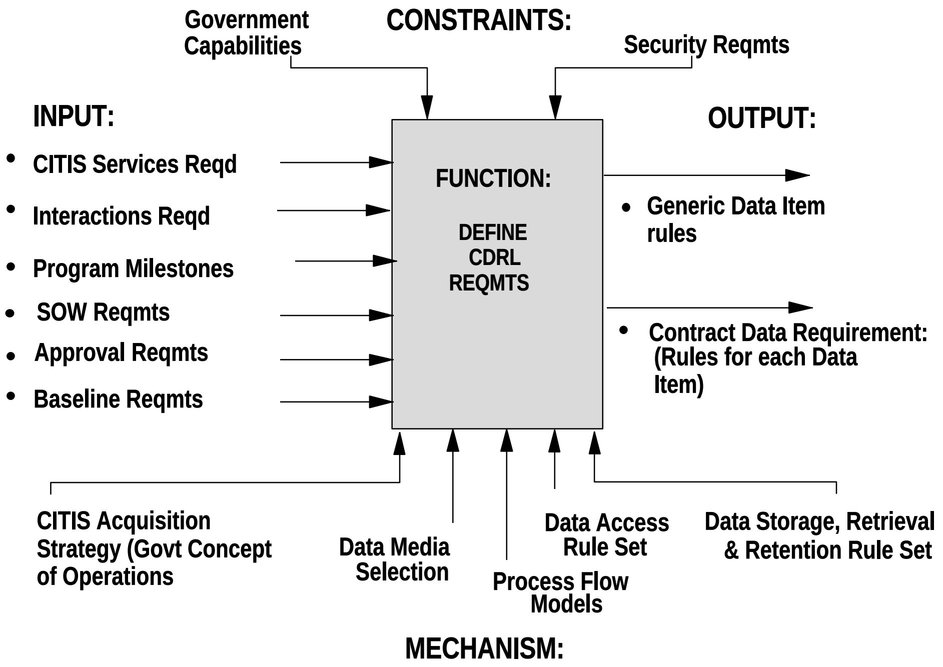

Figure 7-4. *Activity Guide*: CM Data Acquisition Definition Model

Table 7-1. *Activity Guide:* CM Data Acquisition Factors

Type of Factor/ Factor	Description	Considerations, Notes
INPUT		
• CITIS services required	A determination that documents will be required to be made available using Contractor Integrated Technical Information Services	The Government concept of operations and the Contract must call for CITIS services
• Interactions required	The actions that the Government intends to take with each particular type of data.	e.g., View, comment, approve, combine, download, edit, forward, query, sort
• Program milestones	Delivery requirement with respect to specific program events	e.g., 30 days prior to PDR
• SOW requirement	The statement of work task to which the data is associated, or which specifies a data task	
• Approval requirement	If the document(s) submitted pursuant to each CDRL are required to be approved by the Government or are merely for information purposes	Documents that are approved by the Government should be limited to Government configuration baseline documents, wherever possible
• Baseline requirement	Whether the document type when approved will constitute a Government configuration baseline	
CONSTRAINTS		
• Government infrastructure	The capabilities of each of the Government activities which need to view or use the data.	The means of data access (e.g., CITIS, direct input to CMIS, etc.) must be matched to the facilities, equipment and environment of the using community
• Security classification; data rights	Whether the data will be classified and to what levels of classification. Whether the Government anticipates that they will have unlimited rights to the data provided	These factors can influence the processing rules and choices of output media

Table 7-1. *Activity Guide:* CM Data Acquisition Factors

Type of Factor/ Factor	Description	Considerations, Notes
MECHANISMS/FACILITATORS		
• Government Concept of Operations	GCO identifies expected Government infrastructure at all of the participating sites and agencies	Influences services, media and access to be ordered
• Data media selection guidelines	Government preferences for types of media to be used for various document types	Helpful to have a pre-planned priority list of media preferences to match with contractor proposals
• Data work flow process	A work flow process defining the actions that Government will perform on data that is submitted or provided for access	Aides in determining necessary lead time. Documents Government process from submittal by contractor to disposition
• Data access rules	A set of ground rules that is agreed upon with the contractor governing both government and contractor access to data	Use to formulate specific access privileges
OUTPUTS		
• Generic data item rules	Defined set of business rules specific to the program to determine: • Data item life cycle processing • Data naming and revision/version scheme(s) • Means of change annotation revised data • Retention requirements for superseded data • Change authorization process • Validation of transmittal • Times of day/night that data will be accessible for Government use • Requirements for demonstration and certification of sender/receiver compatibility, indexing, accounting and audit trails	These rules apply to all CDRL items
• Specific data item requirements for each CDRL	Specification for the type of document representation required for delivery or access to each CDRL item including, as appropriate: • Media or access mode • Data representation form • Standards, specifications, protocols • If on-line service, the type of query, pre-defined, or ad-hoc • If pre-defined, a specification of or reference to a description of the queries/response formats	These rules apply individually to specific CDRL items